

State of Montana Information Security Advisory Council

Council Meeting Minutes August 16, 2016 11:00 a.m. State Capitol Building - Room 152

Members Present:

Lynne Pizzini, CISO/SITSD, Chair
Dawn Temple, DOJ
Joe Frohlich, SITSD
Bryan Costigan Justice/MATIC

Adrian Irish, U of M
Margaret Kauska, DOR
Craig Stewart, DMA/MNG
☞ Erika Billiet, City of Kalispell

Staff Present:

Jennifer Schofield, Wendy Jackson

Guests Present:

Sean Rivera, Suzi Kruger, Lisa Vasa, Tim Kosena, Jon Straughn, Lance Wetzel, Rebeca Cooper, John Burrell

☞ Real-time Communication:

Phillip English, Anne Kane, Terry Meagher, Michael Jares, John Cross, Christi Mock, Sky Foster, Erin Stroop, Mandi Hinman, Mike Mazanec, Ricky Hale

Welcome and Introductions

Lynn Pizzini welcomed the council to the August 16, 2016 Montana Information Security Advisory Council (MT-ISAC) meeting. All members and guests were introduced.

Minutes

Margaret Kauska made a motion to approve July 21, 2016 minutes as presented. Bryan Costigan seconded the motion. Motion carried.

Business

Update on Phishing Campaign

Lisa Vasa gave an update on the Phishing Campaign. The first phishing messages for this campaign were sent out in August, 2016. The email appeared to come from the State Information Technology Services Division (SITSD) Service Desk. The results for the first phase of the phishing campaign; 736 messages sent. 12 emails bounced (invalid addresses, probably belonging to employees that no longer work for the State). 724 messages were received by the recipients. Of those, 25% of recipients opened the email and 13% of the recipients clicked on the link. Only 1/3 of the individuals who opened the email took the time to read through the landing page and acknowledge the training. 16% of the people who received this message reported that they received it and thought it was phishing. The average open time of the email was within 6 hours of receipt. A large portion of recipients opened the email within the first 30 minutes. Had this been a malicious message, it could have spread very quickly. The SANS, Securing the Human program also indicated what browser the recipients were using and it checked for vulnerable plugins. Over 2/3 of the individuals that clicked on the link had vulnerable plugins in their browser. These included Adobe Flash, Java, Microsoft Silver Light, Quick Time, and Adobe Acrobat. Almost half of the people who clicked the link had outdated Adobe Acrobat. It was recommended that all browsers be kept up to date to reduce threats from vulnerable plugins.

Adrian Irish found it troubling that 75% of the email recipients ignored a message that appeared to have been sent by the SITSD Service Desk. Lisa Vasa replied that these individuals may have recognized the inconsistencies in the email address that would indicate a phishing scam and deleted the email without opening. The address was listed as Service Desk but did not include mt.gov. Lisa Vasa will provide participating agency's with the percentages of their agency's results concerning this training.

Q: Bryan Costigan: Do you have data concerning the amount of time between when the emails were sent and when the first one was opened?

A: Lisa Vasa: I received an email each time when someone would click on the link. I had my first email notification in under five minutes after sending the batch phishing emails out.

Lynn Pizzini noted the sizable improvement in the vulnerability risk assessment, from a 50% click rate in 2014 to a 13% click rate in 2016.

Website Privacy Review

Sean Rivera updated the council on the website privacy review. SITSD was tasked by the State Administrators and Veterans Affairs Committee (SAVA) to check all State of Montana agency websites for a privacy statement link to insure compliance to Montana Code Annotated (MCA) 2-17-505. 170 unique URLs were reviewed. There were approximately 29 findings of compliance issues. Of that, 16 were broken links and 13 were URLs that didn't have a link at all. Sean Rivera has contacted the affected agencies and their respective security contacts asking for remediation. Agencies have been requested to respond by September 30, 2016.

Workgroup Updates

Assessment Workgroup

Joe Frohlich reported that the Assessment Workgroup is working on the Policy Assessment Tool and refining the tool based in the comments received. The second draft will be posted for review during the September 15, 2016 MT-ISAC meeting.

Best Practices / Tools Workgroup

Joe Frohlich informed the council that the Best Practices Workgroup is reviewing the Acceptable Use - Rules of Behavior document. Comments received will be incorporated. Lynne Pizzini stated the document will be updated and reposted for comment. An email vote will be taken or it will be placed on next month's agenda. Joe Frohlich thanked Rebecca Cooper from Fish Wildlife and Parks, Lantz Wetzel from Montana Department of Transportation, and Kurt Fehlig from SITSD for their work on the document.

Motion: Dawn Temple made a motion to approve the Traveling Abroad - Cybersecurity Tips document as a best practice. Margaret Kauska seconded the motion. Motion carried.

Enterprise Endpoint Protection Workgroup

Joe Frohlich updated group on the Request for Information (RFI) for the Enterprise Endpoint Protection Workgroup. That has been posted in SharePoint under Tools. The RFI will go out to the five selected vendors this Friday.

Situational Awareness Workgroup

Bryan Costigan stated that there was no update from the workgroup for this month.

Lynne Pizzini commented that the incident report document was shared with other states in a meeting of Chief Information Security Officers (CISOs). It has been recommended that this form be used on a national level.

Legislature Workgroup

Joe Frohlich stated that Ron Baldwin has agreed to Chair this group and that Adrian Irish and John Burrell will be part of this workgroup. Any other interested parties should email Joe Frohlich at jfrohlich@mt.gov.

Fostering Future Professionals Workgroup

Lynne Pizzini mentioned that the Fostering Future Professionals Workgroup, discussed in last month's meeting, will be formed. Individuals interested in joining this workgroup should email Joe Frohlich at jfrohlich@mt.gov.

Current Threats

Sean Rivera gave a brief presentation. Microsoft has since extended support for Intel Sky Lake Chipset systems up and through the regular end of life cycle (January, 2020 for Windows 7 and January, 2023 for Windows 8.1). This extended support means that patches and the updates are free through those dates. Last week Apple published an update for their iOS system which affects iPhones, iPads, and iPods. It resolves an issue where you can jailbreak the device which thwarts many of the security features that Apple has built in. It also prevents additional malicious codes from being executed on the systems. Finally, researchers have figured out how to break into cars by intercepting the wireless signals of remote keyless entry systems. This particular vulnerability affects millions of Volkswagen, Ford, GM products and various EU vehicle manufacturers. This is accomplished through the use of a battery powered listening device and a signal jamming device. On average it takes one minute to unlock the door. This process is also being sold on the black market. Researchers are skeptical that there is

any kind of simple solution to this. It is estimated that as many as 100 million vehicles may be vulnerable to this type of eavesdropping attack.

Member Forum /Future Agenda Items

None

Public comment

Rebeca Cooper commented that the mini group to edit the Acceptable Use document will meet August 29, 2016. If anyone wishes to make further comments regarding this document, they should upload them as soon as possible so that they may be incorporated into the document by the next council meeting.

Adjournment

Next Meeting

September 15, 2016

11:00 AM - 1:00 PM

State Capitol, Room 152

Adjourn

The meeting adjourned at 11:38 AM.